

# MA357—Introduction to Number Theory

Spring, 2008

Fernando Q. Gouvêa

People have always been fascinated by numbers and their properties, and number theory is the natural outgrowth of that fascination. One finds questions of a “number-theoretical” type already in the mathematics of ancient Greece, India, and China. Since then, number theory has become an important part of the western mathematical tradition. Because it deals with patterns that are easily observed empirically, it sometimes has the feel of experimental science. On the other hand, the proofs that these patterns hold (or that they don’t) are often hidden so deeply that one needs extremely sophisticated mathematical tools to make any progress at all. It is perhaps this blend of simplicity (in the questions) and depth (in the answers) that has led mathematicians such as Gauss to proclaim number theory “the Queen of Mathematics.”

During most of this time, number theory was also famous for being the purest of “pure mathematics.” Even as late as 1982, when Jean Dieudonné wrote his *Panorama of Pure Mathematics* (check it out, it’s in the library), one could claim that there were no contacts between number theory and the physical sciences. That has all changed, quite suddenly, over the last few decades, when two new realms of application became more and more important. The first is computer science, where number theory has come to play a crucial role in the problems of encoding data and of encrypting data. The second is theoretical physics, where recent developments in string theory and related ideas have led to surprising connections with number theory.

Of course, it never was quite true that number theory had no applications: in any situation that is discrete, one is bound to run into number-theoretical problems, and one can mention several examples beginning in the mid-nineteenth century. The difference, I think, is that those examples involved application of relatively elementary number theory, while modern-day applications have grown increasingly subtle and have in fact motivated

new work in the field. This course will pay some attention to the applications of number theory, especially those related to cryptography, but our main focus will be on the theory itself. Nevertheless, I will try to give you pointers to significant applications as we reach the relevant portions of the course.

So what is number theory about? It is about numbers, but in a special sense. Number theory isn't really too interested in specific problems about particular numbers (that's arithmetic); instead, it focuses on broad, general patterns, and particularly on patterns that are not immediately obvious but can be discovered by careful investigation. We will discuss a number of questions of this type in our first class meeting.

This course will be an introduction to elementary number theory. The word "elementary" here has a technical meaning: it indicates that we won't be using more advanced theories (such as complex analysis or algebraic geometry) to study number-theoretical patterns. This means the course has few pre-requisites, but it does *not* mean that the material is easy — in fact, many of the theorems we'll be thinking about are quite subtle.

I think number theory is fun. I hope you'll come to agree.

**Office hours:** I will be in my office and available for questions, discussion, and general conversation on Mondays, Wednesdays, and Fridays from 1:00 to 3:00. If you can't come during any of these times, please call and make an appointment.

Please do not hesitate to come see me — in fact, I strongly encourage you to come. It is part of your education, and one of your privileges as a Colby student.

**Where to find me:** The mathematics department no longer fits in the fourth floor of the Mudd building. The college has promised us space in a new academic building, but that's still in the future. Meanwhile, someone had to be exiled, and I volunteered. So my office is in the Olin building. I get lonely there... do come visit!

office: Olin 342

phone: 5836

email: fgouvea

If you need to reach me when I'm not in my office, email is the best method. I'm usually pretty quick at answering email.

**Texts:** Our textbook will be *A Friendly Introduction to Number Theory*, by Joseph H. Silverman. I hope you'll find it both readable and pleasant. We have a second required book, John Derbyshire's *Prime Obsession*. This is not a textbook; rather, it's a "popular math" book. That doesn't mean it's easy, but I hope you'll find it readable. In a first course in Number Theory, we inevitably have to spend a long time on the foundations of the subject. This is fine (and, I hope, interesting), but it doesn't really give you much of a hint of what the outer reaches are like. Derbyshire's book will give us a glimpse of one of the branches of more advanced number theory (what is known as "analytic number theory").

**Other books:** It's important to remember that Colby does have a good library. We have many books on number theory, and it's quite possible that one of them will fit your personal style and so prove to be a useful complement to Silverman. The number theory books live in the sections of the library numbered QA241-247.

Finding another book to work with is particularly important if you have already taken a few theoretical math courses and would like a more formal and more detailed text. If so, please *do* find such a book to consult and work with. The books by Davenport, Hardy and Wright, Niven and Zuckerman, Sierpinski, Baker, Cohen (a two-volume monster) and Hua Loo Keng all would fit the bill. There is also *The Book of Numbers*, by Conway and Guy, that presents itself very informally but is really quite serious.

A different set of books would be relevant to those of you who are interested in computer science. Pride of place goes to the book by Bressoud and Wagon, which uses *Mathematica* to explore the properties of numbers. Also interesting are the books by Bach and Shallit, Crandall and Pomerance, and Riesel.

The number theory I'm most interested in has an *algebraic* flavor (in the sense of abstract algebra). One of the best starting places to learn more about that is *A Classical Introduction to Modern Number Theory*, by Ireland and Rosen. See also the books by Murty, Neukirch, Stewart-Tall, and, if you like an historical approach, Edwards.

It might be fun to look at books that highlight the applications of Number Theory. For example, *Number Theory in Science and Communication*, by M. R. Schroeder, *The Unreasonable Effectiveness of Number Theory*, ed. by S. Burr, *From Number Theory to Physics*, ed. by M. Waldschmidt et. al., and pretty much any book on cryptography.

In other words, whatever your interests, don't limit yourself to the required books. Go explore. Read the introductions. Read a few chapters. Skip over uninteresting details. Have fun. If you like, ask me for further suggestions of things to read.

**Web site :** Our course web site is at

<http://www.colby.edu/personal/fqgouvea/357>

Go there. I'll try to post all the course handouts and other interesting stuff.

**Technology:** Number theory has an experimental side: one can detect number patterns by computing a large number of examples. You will probably find it useful to use either a calculator or a computer to construct examples, test conjectures, and experiment. For the first part of the course, a calculator may be sufficient (but if your calculator doesn't do infinite-precision arithmetic you should watch out for rounding errors). To deal with bigger numbers, however, one absolutely needs to use a computer program that can do integer arithmetic. If you're familiar with *Mathematica*, you're welcome to use that. What I really recommend, however, is a program called GP, which is a kind of "calculator" geared to number theory. It's a free program, so you can download and install your own copy if you want to use it. I've put some information on this program on the web: go to <http://www.colby.edu/personal/fqgouvea/357>.

**Assignments:** There will be a variety of assignments during the course:

- **Automathography by email:** your first assignment is to send me a short email message introducing your mathematical self to me. Tell me about courses you have taken, about ideas that you've found exciting, about things you've found boring or difficult, about your goals as a student. If you have taken MA274, I'd like to know what that was like and how much you remember. If you have worries about any special problems or needs, let me know. You are encouraged to be creative in your response; don't just answer the questions above, but include whatever else you wish. This email message is due no later than **Monday, February 11**.

- **First writing assignment: review a book.** There will be two writing assignments. The first will be based on John Derbyshire's *Prime Obsession*. You will be asked to read the book and then write a review. Your review should describe the content of the book, discuss the quality of the expository writing, and give your reaction to both the mathematics and the history that Derbyshire explains. More details about this assignment will be provided during the first week of classes. This assignment will be due **Friday, March 7**.
- **Second writing assignment: a mathematical exploration.** The second writing assignment will involve some expository mathematical writing of your own. I will provide you with a list of possible topics, all of which will consist either of a significant theorem or a problem (solved or unsolved) that requires some exploration. (It's ok for you to choose your own topic, of course, but check with me first.) This paper has a dual goal: to understand a small bit of mathematics as thoroughly as possible, and then to explain it as clearly as possible. More details of this assignment will be provided later. This assignment will be due **Friday, April 25**.
- **Problem Sets:** Problem sets will be passed out **every Friday beginning on February 8** and will be **due the following Friday**. These will include a few routine practice problems and a few more interesting problems that will require some thought and creativity. These problem sets *will* take several days to complete: don't leave them for the last day! See the handout *On Writing Up* for information on what is expected and on how these assignments will be graded.

**Exams:** We will have one midterm exam, in the second week of March, and also a final exam. Both exams will be take-home exams. I will provide more information as we get nearer to the exam dates.

**Grading:** Your grade will be computed as follows:

problem sets	20%
writing assignments	30%
midterm exam	20%
final exam	30%

**Attendance:** You are expected to come to class. Should you be unable to come to class on a particular day, please contact me. Unexcused absences *will* have an effect on your grade for the course. As per college rules, many unexcused absences may lead to your being asked to withdraw from the course.

**Cheating and Plagiarism:** You are encouraged to interact with others as you do your assignments (in fact, it will be a lot more fun doing it that way). The written work that you turn in, however, must be your own. You may, of course, seek help from any and all sources, but in the end what you write must be a result of your own thought processes and your grappling with the material. Feel free to discuss any questions you have about this with me. Also, please read the Colby policy on academic honesty as stated in the College Catalogue.

**On reading your textbook:** I expect you to read your textbook. This doesn't mean that you have to learn everything by yourself, but it does mean that I will often concentrate on the central ideas of an argument when the book contains all the details. Of course, you should feel free to ask questions about what's in the book when we discuss the material in class.

Reading a mathematics book is not like reading other texts. First of all, it's slow. Mathematicians tend to write in a very compressed, terse style, and reading it takes lots of "unpacking." As you read, have paper and pencil in hand, and be careful to work out examples, fill in details, check assertions. Second, one reading is not going to be enough. I suggest that before each class you try to read the relevant sections of the book. In this first reading, you should try to get the overall structure of the argument, without worrying too much about the details. Then, after class, re-read the section, comparing with what we discussed in class and filling in all the details you can. If necessary, compare with other books. Discuss the material with other people, and with me. Then read again.

**Working with others:** Mathematics is a social activity. Mathematicians are always talking to each other, explaining questions and theorems and saying things like "what's really going on here is...", "do you know whether..." and "I have a conjecture..." You'll enjoy this course more if you can find a small group of people to work with, not only doing the homework together, but talking about the material. The more you invest, the more you'll profit.

**A tentative schedule:** Here is the tentative schedule, with a list of readings for each week. This is very ambitious, and I won't hesitate to change it as we go along, but I hope it will give you some idea of what we will be covering and of what to read in preparation for each class.

- Feb. 6–8** Introduction, Pythagorean triples. (chapters 1–4)
- Feb. 11–15** Divisibility, gcd, linear diophantine equations (chapters 5, 6)
- Feb. 18–22** Factorization, congruences, Fermat's Little Theorem (chapters 7–9)
- Feb. 25–29** Euler's theorem, the  $\phi$  function (chapters 10, 11, 19)
- Mar. 3–7** Primes and their distribution, (chapters 12, 13, *Prime Obsession*).  
First writing assignment due on Friday.
- Mar. 10–14** Mersenne primes, perfect numbers (chapters 14, 15)
- Mar. 17–21** Powers modulo  $m$ , roots modulo  $m$ , and applications to cryptography (chapters 16–18)
- Mar. 24–28** Spring Break
- Mar. 31–Apr. 4** Primitive roots, indices (chapters 20, 21)
- Apr. 7–11** Squares modulo  $p$ , quadratic reciprocity (chapters 22–24)
- Apr. 14–18** Sums of two squares, sums of fourth powers (chapters 25–27)
- Apr. 21–25** Pell's equation and diophantine approximation (chapters 29–31)
- Apr. 28–May 2** Cubic curves and elliptic curves (chapters 40–41)
- May 5–9** Elliptic curves continued, wrap-up (chapters 42–45)

